Montana Information Security Advisory Council
Meeting Minutes

October 21, 2015
Montana State Capitol, Room 152
1:00 pm – 3:00 pm

Attendee’s	
Special Guest: Governor Steve Bullock	
Meeting Chairperson: Ron Baldwin, State CIO	
Name	**Affiliation**
Erika Billiet	**City of Kalispell**
Joe Chapman	**Department of Justice**
Bryan Costigan	**MATIC/Department of Justice**
John Daugherty	**Department of Corrections**
🖱**Sherri Davidoff**	**LMG Security**
Kreh Germaine	**Department of Natural Resources and Conservation**
Jim Gietzen	**Office of Public Instruction**
Adrian Irish	**University of Montana**
Margaret Kauska	**Department of Revenue**
Representative Kelly McCarthy	**(D) HD 49**
Lynne Pizzini	**State Information Technology Services Division**
Major General Matthew Quinn	**Director of Military Affairs, Montana National Guard**
Meeting Minutes recorded by: Samantha Cooley	

Meeting Guests: Joe Frohlich, SITSD; Bill Genzoli, ATOSI/Xerox; Lance Wetzel, MDT; Sean Rivera, SITSD; Carroll Benjamin, and BG Bryan Fox, DMA

🖱**Online Attendees:** Brad Flath, Dawn Temple and Terry Meagher

I. Welcome and Introductions

Today’s meeting is a special occasion. Governor Bullock will be joining the group at 2:30. In addition, the Enterprise Security Program is holding a Cybersecurity Awareness Training Event upstairs. The Council will have the option to attend during break.

Approval of September Meeting Minutes: The September, 2015 MT-ISAC Meeting Minutes were approved and accepted as written.

Motion: Bryan Costigan motioned to accept the minutes, Lynne Pizzini seconded the motion. All were in favor. The motion carries.

September Meeting Recap
The September meeting was very productive. The Goals and Objectives were approved, the Baseline Security Controls were discussed and Mike Manion provided his legal opinion on the adoption of the Five Enterprise Security Policies.

II. Enterprise Security Policy Discussion-Appendix D, Joe Frohlich

Background
At the September meeting the language for the Five Enterprise Security Policies and the updated appendices A, B, and C were approved. There was some uncertainty regarding obtaining compliance with two separate documents, the Five Enterprise Security Policies and the Baseline Controls. It was recommended by the Council that the two be linked together and that one policy would be easier to comply with than six. Therefore, all five policies were merged into one final "Information Security Policy" document that contains sections for each core security function and all of the supporting appendices: A, B, C and D. The MOM listing of this policy is: POL-Information Security Policy.

Purpose: Appendix D was created to link the Five Enterprise Security Policies and Baseline Controls together. This document is posted online.

Layout
Appendix D lists the functions (Identify, Protect, Detect, Respond, and Recover) and bridges those back to the Baseline Security Controls. The categories that fall within each function are listed in column two and the crosswalk to NIST/Baseline Controls is listed in column three. The paragraphs supporting the core security functions were changed from an alphanumeric outline to a decimal outline, for ease of identification. The language has not changed, only the numbering in the outline.

Section F-Implementation
Section F-Implementation is a new section and was recommended by the Council at the September meeting. This addition states:

> *'All state agencies will implement the controls identified in this policy within a three to five year timeframe. Agencies will provide status updates on implementation progress to the CIO in July of each year for the prior fiscal year.'*

Feedback
Kreh Germaine commented the new policy is nicely organized and well put together. It is packaged in a way that makes it easy to grab ahold of.

Lynne Pizzini thanked Joe Frohlich for his effort in putting this together.

Bryan Costigan commented that overall the crosswalks will help everyone find what they need to find quickly.

Next Steps
The Information Security Policy is still in draft. DOA Director, Sheila Hogan and State CIO, Ron Baldwin will need to sign a decision brief to officially approve the policy. After the draft has been approved it will be available as a template for agency use.

Ron Baldwin walked through the policy with Lynne and Joe and feels it is well organized and is a model policy for other States. The minutes from the last meeting contained some excellent suggestions on implementing this policy Statewide and addressed some of the liability concerns that

Chief Legal Counsel, Mike Manion, spoke about. Ron thanked Sheri Davidoff for her suggestion on implementation.

The policy is organized in one package that agencies can rely on completely as a template to meet their specific needs and largely, points back to the bedrock and foundation of the work this Council is doing. Taking the Council's advice and work into consideration, Ron believes the policy will be approved.

Inquiry, Kreh Germaine:

> *"I was looking through the document earlier and was curious if SITSD, or any other agency, has measured the amount resources needed to implement this policy. Has that been done? If not, can we do that?"*

Response, Joe Frohlich:

> *"I think that would be an item the Best Practices Workgroup can address."*

Response, Ron Baldwin:

> *"My thought is that this group can create a template work-plan that includes a series of tasks that can be resourced. Those resources would depend on the agency and would scale out the resources needed for each agency depending on their scope. My recommendation is that the Best Practices Workgroup puts together a framework work-plan template that would be used to determine the resources needed for each agency."*

OPI has just stared this process internally. They have developed a high level plan that estimates the process will be complete within four years. They will begin chipping away at it section by section until it's finished. OPI is very limited with their resources, but that is how they are going to approach it. Jim Gietzen, or one of his delegates, will be on the Best Practices Workgroup.

Stuart Fuller commented that HHS has done a lot of work with Michael Barbere, SITSD, because of the review on their security posture. Stuart feels they have a good outline on their framework and would be willing to share his process with Kreh and/or the Best Practices Workgroup. Concerning the number of FTE it will take, it is a larger number than one would think and is a larger number, unfortunately, than one will get.

Kreh Germaine commented that knowing what resource estimates might look like by next session would be helpful.

III. <u>Rescinding 28 Security Policies, Joe Frohlich</u>

At the last meeting it was approved to merge the 28 policies into Appendix A. Joe listed each policy on the screen, today's action item is to rescind these policies from MOM now that they have been consolidated into Appendix A.

Stuart Fuller expressed concern that HHS needs to have security policies in place to report back to Federal partners that require policies to exist. Replacement policies will need to be enacted at the same time. Joe Frohlich reassured Stuart that Appendix A has already been approved and this will not be a problem, given there is no gap.

Motion: Lynne Pizzini motioned to rescind the 28 Security Policies listed. Bryan Costigan seconded the motion. All were in Favor. The motion carries.

IV. Formation of Suggested Workgroups, Joe Frohlich

At the last meeting the Council approved the Goals and Objectives Workgroup and compiled a list of potential workgroups to be voted on via email. Joe sent a survey to the group and projected the survey results on the screen. The survey asked each Council Member to rank the workgroups in two ways:

1. *What is most interesting to you as a Council member?*
2. *What is necessary to accomplish the Goals and Objectives established for MT-ISAC?*

A summary of the responses is listed below.

Survey Question 1: Rank the workgroups in order that most interest you.

13 respondents, items listed from highest rating to lowest rating.

1. Best Practices
2. Situational Awareness
3. Assessment
4. Legislative
5. Resources
6. Tools
7. Awareness & Training
8. Fostering Future Security Professionals
9. Public Safety
10. Outreach

Survey Question 2: Please rank the workgroups in order as you see them necessary to accomplish the Goals and Objectives.

13 respondents, items listed from highest rating to lowest rating.

1. Awareness & Training *and* Best Practices (tie score of 7.38)
2. Assessment
3. Tools
4. Situational Awareness
5. Resources
6. Legislative
7. Outreach
8. Public Safety
9. Fostering Future Security Professionals

Discussion

- Awareness and Training is already being handled well by the Enterprise Security Program, there is no need to have a Workgroup for this area. It was recommended by Joe Chapman that they report in to the Council with progress on a regular basis.
- The Best Practices Workgroup was identified as a critical and high priority workgroup.
- MT-ISAC Meetings will be the primary forum from which the MT-ISAC Workgroups share information/progress and communicate with one another.
- It was suggested that the Tools Workgroup be merged with Best Practices Workgroup, although the group decided to keep the two separate for now.

- The Assessment Workgroup was identified as a critical and high priority workgroup.
- The Assessment Workgroup will do the following:
    a. Focus on developing a plan of action and milestones to accomplish compliance with the Information Security Policy
    b. Create a template that can be used Statewide to promote uniform reporting on security posture
- In order to keep their focus, the workgroups should remain separate for the time being.
- Three MT-ISAC workgroups is a good number of workgroups to start with.
- Sherri Davidoff and Major General Quinn will work informally on the Cyber Environment Workgroup and will serve on that committee once it is official.

Outcome: Situational Awareness, Best Practices and Assessment will be the operating workgroups for MT-ISAC.

Workgroup Name	**Chairperson**	**Members**
Situational Awareness	Bryan Costigan	Bryan Costigan, Joe Frohlich, John Burrell, Lynne Pizzini, Sean Rivera, Bryan Fox, Craig Stewart, Joe Chapman, Dawn Temple, Suzi Kruger, Bill Genzoli, Judy Kelly
Best Practices	Lynne Pizzini	Jim Gietzen, Margaret Kauska, John Daugherty, Stuart Fuller
Assessment	Lynne Pizzini	Joe Frohlich, Major General Quinn, John Daugherty, Kreh Germaine, Sherri Davidoff

V. <u>Workgroup Updates</u>

Situational Awareness Workgroup Update, Bryan Costigan

Progress: The group has met since the September MT-ISAC Meeting. The meeting was spent going through and developing standing information needs. The questions developed will be used as a tool to provide information.

Next Steps: There will be a meeting next Wednesday to start working on how information collected will be disseminated and what products will be used to disseminate out to everyone in State Government, with an eye leaning towards the private sector. The initial focus will be on the State agencies, later they will determine what they can share with the private sector. The final piece is how to receive reporting, from the group, as the information broker.

Inquiry, Major General Quinn:

> *"If you receive information from a private sector seeing increased activity, are you able to share that information with the MT-ISAC, even by anonymizing it?*"

Response, Bryan Costigan:

> *"Yes. That is exactly how it goes. The information will be anonymized, it will say 'a Montana based corporation had X, Y, and Z and happen to it'. Furthermore, it can be made to identify a certain sector, for example, a utilities corporation. On a larger scale,*

there are ISAC's for all of the critical infrastructure pieces, which is probably where the information will be funneled. We would probably end up writing an IIR Information Report that would hit the ISAC's. They would report out and we would report out."

Inquiry, Major General Quinn:

"*If we receive information that a critical infrastructure may be under cyberattack, does that have to be released under Montana's public disclosure law if DHS deems it critical information not releasable at the Federal level*?"

Response, Bryan Costigan:

"Some of it is protected Federally under protected critical infrastructure information in a specific statute."

Inquiry, Major General Quinn:

"Can Montana also protect this information? This is something that is being asked by the National Governors Association to all Homeland Security Advisors. Can it be protected in Montana by Montana's Public Nondisclosure Law?"

Response, Bryan Costigan:

"*Yes, it is considered criminal activity, because it is an attempted intrusion which is a violation of Montana Code Annotated, its confidential criminal justice information."*

Inquiry, Major General Quinn:

"Do you have an analysis on that? They are asking how each State derived that to be protected or not protected."

Response, Bryan Costigan:

"*We sat down and went through all of these, the current Governor was involved in the process. In addition, there is another statute that protects critical infrastructure information that has to do more with plans. For example, the Northwestern Energy grid."*

Response, Stuart Fuller:

"There is an MCA that relates to the protection of security information, for example, a prison blueprint or the configuration of the State's firewall."

VI. <u>October Cybersecurity Month</u>

VII. <u>Joint Task Force on Fraud and Identity Theft Update , Margaret Kauska</u>

Margaret thanked Joe Frohlich for attending/assisting with the last Joint Task Force on Fraud and Identify Theft Meeting. DOR is spearheading this effort on identity theft and fraud by working with agencies to protect citizens of Montana.

The group, to date, has had two meetings. At the last meeting they talked about the war on identity theft. Lee Baerlocher shared an IRS identity theft video from CSB news which was both enlightening and frightening. DOR wants to be able to share information with agencies as much as they can, they are protected by State statute, however, several agencies have their own, unique Federal statutes to which they must comply.

Margaret put together a document that outlines what information DOR is allowed to share. Some of the information comes from memorandums of understanding, Title 15 also allows them to share certain information. However, they want to be able to share more and be able to obtain information from agencies to reduce fraud and identity theft in Montana. The discussion led to a need for a common identifier that can be used across the Enterprise to identify cases, social security numbers cannot be used.

At the meeting, Joe Frohlich was asked if there is something that can be done at the Enterprise level to determine how to share information without breaching any laws and protecting citizens. It’s a good group, they have had a lot of good conversation.

Bryan Costigan stated that the whole idea on information, on what the State can and cannot share, came to a head the other day. An issue came up with an employee that was removing information and storing it improperly and possibly illegally. The police department came in, however, due to agency personnel policies, it was difficult for the police to follow through. The police were not able to interview witnesses as needed and as quickly as it should have been done. These issues should be worked through before a crime occurs. DOR has constraints with the IRS, DPHHS has constraints with HIPPA. However, when something is reported, the police need to be able to do their job. This is especially true with computer crimes. Information should be obtained as quickly as possible.

Margaret Kauska commented that the situation Bryan is referencing affected more than just DOR and because of laws on information sharing for other agencies, it has not been a very efficient process. It was difficult to get through all of this, working within our own statutes when time is of the essence.

Mitigation of the issue is of concern. If there is someone stealing information, and utilizing that information, if the potential victim cannot be identified, it can’t be stopped. The more time that passes, the less likely it will be stopped.

Inquiry, Major General Quinn:

> *“Is the Task Force going to come up with a policy for the agencies that will say if this happens, here is how you can comply with law enforcement?”*

Response, Bryan Costigan:

> *“In general, it can be hard because of all of the different holders of the information. There is HIPPA with DPHHS and even with the Guard, there is a lot of information there.”*

Major Quinn commented he would be looking for something on the State side that says, for those of you not covered under IRS or HIPPA, here is an example of how you can cooperate. There is enough of us that something like that would be helpful.

Action: Margaret Kauska will ask Lee about developing a policy that is an example for agencies on how to comply with law enforcement when a potential cyber-crime occurs.

Inquiry, Representative McCarthy:

> *"What would trigger you to share information? I have had five tax returns fraudulently filed on my name this year, they were caught. Does that go to some central clearing house where it's flagged for the next State that receives it?"*

Response, Margaret Kauska:

> ***"****Actually, yes, because identity theft and everything that is going on, we as states talk weekly or bi-weekly. We have different Task Forces, committees and Suspicious Filer Programs. We can share information within the confines of our own State statute. It is something that every State, as well as the IRS is very aware of. What triggers sharing is if we get notice from another State, we are allowed to share information. We have an agreement through the Multistate Tax Commission and Federation of Tax Administrators that provides a network where trends and situations can be discussed. With the upcoming filing season coming, we are all very aware of trying to be more cautious. As returns start coming in and we notice certain trends, we certainly share that information."*

The number of fraud cases continues to be on the rise. Montana DOR is catching more cases than they ever have because they are currently on high alert. Last year, they took precaution to slow down refunds so they could ensure refunds were going to the right people.

Action: Margaret will bring in the figures on the rise in fraud in Montana, how much DOR is catching vs. what is missed.

Fraud Cross-Over Cases

Bryan commented that another concern is that there are other benefits available through the State. There are cases where there is cross over between benefit programs. For example, someone might commit tax fraud during filing season and then switch over to unemployment fraud. One person can commit a multitude of frauds. The State needs to be able to identify them in multiple places.

The discussion about an identification number spawned from that conversation. Something needs to be in place that can hook all these people together, without using the social security number.

Unique Identifier

John Daugherty commented he is in support of the unique identifier. Using a social security number requires a lengthy MOU process. If another way can be identified, it would make this a lot easier. Stuart Fuller commented that even within DPHHS, there are restrictions between programs and limitations on the sharing of data. There are very strict Federal rules. For example, there are things that can be done in Medicaid but cannot be done in TANF, even within the combined eligibility system, there are limitations. Even the Federal Government doesn't have this dialed where we have this useful information data sharing. This is something they are working on within the Department.

This is an ongoing struggle. One key thing the State needs is to have a discussion on how to implement a unique identifier that is not the social security number.

Kuddos to DOR!

A report done last year by KTVH, in an interview with DOR Director, Mike Kaddus, stated that since tax season started on January 20, the Department had already stopped $26K in fraudulent refunds. The previous year the Department stopped approximately $1.5M in fraudulent refunds.

Thank you to Margaret Kauska and Bryan Costigan for their contributions regarding the Joint Task Force on Fraud and Identity Theft.

VIII. <u>Current Threats, Sean Rivera</u>

Windows 10 Security Features

- **Device Guard:** this gives organizations the ability to lock down devices similar to application whitelisting feature. It looks for signatures and signed applications from vendors and the Windows App Store. It helps to block script-based malware.
- **Windows Hello and Passport:** Users can say goodbye to passwords. Users can log in and authenticate by sitting in front of their computers using the camera system. It uses biometric components such as iris scanning, fingerprint scanning and facial recognition software. The product is very effective. In independent testing some technology bloggers sat down six pairs of identical twins in front of a facial recognition camera set up with Windows Hello. The copy of the twin was never able to log in based on facial recognition. It will be interesting to see how this works with the Enterprise.
- **Windows Passport:** lets you authenticate into applications and websites through the use of biometrics. It uses a public/private key pair to log into applications and websites. To ensure the end user is in control Windows Passport will ensure authentication by a pin or through Windows Hello.
- **Enterprise Data Protection**: this has not yet been released to Enterprise businesses for user testing. It works similar to MDM and BYOD as far as containerization. Personal and business documents are separated and encrypted throughout the entire use cycle. As that becomes available over the next couple of quarters SITSD will be able to test out further with that.

Visit from Governor Bullock

> *"I just wanted to stop in and give you all thanks for the work you are doing on this. We know that certainly every single day, both in the private and public sector, we are now using technology that much more… hopefully to provide the services we do in State government, but also to make our lives that much easier. On the same token, it also causes significant risk and significant challenge. On the one hand it's easy to try and utilize the technology for all of its opportunities, I think that means we have to be that much more vigilant when it comes to potential threats. I think that when properly constituted this can be an incredible Council because not only does it have*

> *representatives for State and local governments and the private sector, but then also all of the supporting agencies. From DES, to Homeland Security and everywhere else. My main reason for popping by is nothing more than to thank you for the work you are doing. I think this one of these where it is significant as we look forward. I, as the Governor, have seen what more that we at the State level ought to be doing. I will lean on and rely on you all for that advice to make sure we are best protecting ourselves and serving the State as we should. I wanted to come down and thank you."* –Governor Bullock

> *"Thank you Governor for doing that, this Council has already done some amazing including with policy that is going to impact the entire State of Montana."* – Ron Baldwin

IX. <u>Open Forum</u>

Announcements

The Cybersecurity Training upstairs is open today until 4:00 PM.

Calendar invites for MT-ISAC Meetings will be resent to everyone due to staff changes. The new invitation will come from Joe Frohlich.

Workgroup Reporting

The Workgroups will regularly report on their status at each MT-ISAC Meeting. That might include a work plan, any work products the group has created and any issues the group may need to address in that process. The three Workgroups will be added to the MT-ISAC Agenda as a standing agenda item.

Future Agenda Items

Major General Quinn's team is scheduled for their trip to Washington on November 19-20 to look at the Washington Cyber Team. He will report back to the committee upon his return.

Best Practices Workgroup Report (standing)

Situational Awareness Workgroup Report (standing)

Assessment Workgroup Report (standing)

Data Breach Policy for Idaho Juvenile COR

John Daugherty received a request from the Idaho Juvenile Department of Corrections who are looking for agencies in Montana and surrounding states that may be able to provide them with policies/communications plan they could use surrounding data breach. Joe Frohlich commented he has an incident response plan that should work for what John is requesting.

Action: Joe Frohlich will send the incident response plan to John Daugherty.

Aligning the December Meeting with the State IT Conference

Adrian Irish asked if there is any possibility of aligning the December Meeting with the State IT Conference. For members of the Council that are traveling, it would be ideal to make only one trip.

Action: SITSD will look into scheduling the December MT-ISAC during the same week of the State IT Conference and report back at the November meeting.

X. Adjourn

The meeting adjourned at 2:49 pm.

Next Meeting Information
Meeting Date: Wednesday, November 18, 2015
Meeting Time: 1:00 pm
Meeting Location: Montana State Capitol, room 152

XI. Summary of Motions Passed

Motion: Bryan Costigan motioned to accept the minutes, Lynne Pizzini seconded the motion. All were in favor. The motion carries.

Motion: Lynne Pizzini motioned to rescind the 28 Security Policies listed. Bryan Costigan seconded the motion. All were in Favor. The motion carries.

XII. Summary of Action Items

Action: Margaret Kauska will ask Lee about developing a policy that is an example for agencies on how to comply with law enforcement when a potential cyber-crime occurs.

Action: Margaret will bring in the figures on the rise of fraud in Montana.

Action: Joe Frohlich will send the incident response plan to John Daugherty.

Action: SITSD will look into scheduling the December MT-ISAC during the same week of the State IT Conference and report back at the November meeting.

Meeting Minutes draft submitted by: Samantha Cooley on November 9, 2015